CLAIMS

1. A method of providing and managing secure access to computer resources from an external source, the method including the steps of :-

a) receiving a message from said external source at an authorisation check module,

b) requesting credentials from the external source,

c) sending the message and credentials to a session management module,

d) checking the credentials of the external source, and, if valid, issuing a ticket to the external source, the ticket being valid for a plurality of trusted computer systems,

e) receiving a further message together with said ticket from said external source at said authorisation check module,

f) checking the validity of the ticket via the session management module, and

g) passing the message and ticket to an impersonator module which provides secure communication between the external source and the desired destination computer system or resource, the impersonator module also providing usage information to the session management module.

2. A method as claimed in claim 1 in which secure access is provided to a plurality of trusted computer systems or resources.

3. A method as claimed in claim 2 in which the trustworthiness of each destination computer system or resource is established using a cryptographic methodology in which the public key characteristic of an internal computer system and the public key of the external destination computer system or resource are exchanged over a non-secure channel.

4. Computer apparatus connected to a network adapted to perform a method as claimed in claim 1.

5. Computer apparatus connected to a network adapted to perform a method as claimed in claim 2.

6. Computer apparatus connected to a network adapted to perform a method as claimed in claim 3.

7. Computer apparatus as claimed in claim 4, 5 or 6 including a user management module comprising a meta directory in the form of a global user profile database which controls a plurality of LDAP compliant directories.